IT (ADP) Classification Categories

PS-IP-4

September 2003

Personnel Security

TRICARE

Mailing Address

Privacy Office
TMA

5111
Leesburg Pike
Suite 810
Falls Church,
VA 22041

TMA is committed to the protection of patient and sensitive data it is entrusted with, while at the same time striving to make appropriate and lawful access to that information possible in order to fulfill the DoD MHS mission. One measure to protect the use and disclosure of this information is the requirement of background investigations on all personnel with access to sensitive but unclassified information and related information systems. This paper specifically discusses IT (ADP) classification categories.

Why must contractors apply for IT (ADP) levels of trust?

The Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), and the *DoD Health Information Privacy Regulation* (DoD 6025.18-R) along with the DoD 5200.2R *Personnel Security Program* (January 1987), the DoD 5200.2R *Personnel Security Program* (draft June 2002), and the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) require that the DoD put in place appropriate safeguards to protect sensitive data. These safeguards against inappropriate use and disclosure must be upheld by contractors and others who have access to information systems containing protected health information. Background checks for all personnel who will obtain access to systems holding sensitive but unclassified (SBU) data are one method of protection employed by DoD. SBU data is an informal designation for all information that, by law or regulation, requires some form of protection but is outside of a formal system for classifying national security information.

What are some examples of IT (ADP) positions that require levels of trust?

The following are typical category assignments for each IT specialty title defined in the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200" (See http://www.opm.gov/FEDCLASS/gs2200a.pdf for additional information). Other IT-related positions should be categorized based on the particular set of duties and responsibilities of the position and the scope, and level of privileges authorized.

- Security– IT-I (IT-II if primarily policy, planning or awareness focused)
- Applications Software– IT-I, -II, or –III depending on specifics of application (IT-I if responsible for information security/ information assurance applications)

- adp.mail@tma.osd.mil -

IT (ADP) Classification Categories

PS-IP-4

Mailing Address

Privacy Office
TMA

5111
Leesburg Pike
Suite 810
Falls Church,
VA 22041

- Network Services – IT-I or IT-II (depending on the scope of network—as defined by criticality of or impact on Department or Federal government mission, geographic reach, and/or major or significant impact on other government agencies and/or the private sector—and level of privileges)
- Systems Administration– IT-I (IT-II if stand-alone system or if ability to compromise limited to system/network operation)
- Operating Systems– IT-II (IT-I if incumbent acts independently, without oversight/review)
- Internet– IT-II (IT-I if privileged access to network functions)
- Policy and Planning – IT-III (IT-II if responsible for information security/information assurance program or if individual also has privileged access)
- Systems Analysis– IT-III (IT-II if responsible for information security/information assurance systems)
- Data Management– IT-III (IT-II if responsible for safeguarding sensitive data/information)
- Customer Support – IT-III (IT-I if privileged access; or IT-II if ability to set/change user access privileges (scope and level sensitive)

- **Other activities or specialties that may have significant IT duties include the following**:
- Computer Clerk and Assistant or Computer Operation– typically IT-III, but may be higher if there is access to system/network control functions.
- Computer engineer– generally hardware focused; typically IT-III, but specific categorization depends on function and application of the specific hardware/component (e.g., chip/board design may be IT-I), degree of supervision/review by higher authority, etc.
- Criminal Investigating– Law enforcement activities associated with computer/network crime (e.g., forensic analysis; criminal investigation) – categorization depends upon required level of access (e.g., privileged/non-privileged).
- Miscellaneous Management and Program Analysis and other scientists, subject matter experts, and professionals — depends upon required level of access (e.g., privileged/non-privileged).
- Technical editors and other subject matter experts who develop web pages, but whose primary expertise is not technical knowledge of Internet systems, services, and technologies –

IT (ADP) Classification Categories

Mailing Address

Privacy Office
TMA

5111
Leesburg Pike
Suite 810
Falls Church,
VA 22041

categorize under "Internet" IT specialty; if non-privileged access, may be assigned IT-III designation

- Miscellaneous IT specialists (As required by specifics of new technology/evolving specialty area) – use appropriate IT specialty
- Threat and vulnerability assessment (e.g., red-teams; penetration testing) - determined by the purpose and scope of the assessment objective and required level of access.
- Certificate Management Authorities (CMA) to include Verifying Officials (VO) - typically IT-II, but may be higher if operating CMA equipment associated with Public Key Infrastructure operating above the DoD Class 4 assurance level.